1. (currently amended) A method comprising the acts of:

providing an endorsement key pair to a security module associated with a customer computing device, the endorsement key pair including a public key and a private key;

storing data representative of the public key in a storage external to the customer device;

at a subsequent time, receiving at a comparison agent operatively connected to the storage, certificate request data from the customer device, the certificate request data including ~~at least one of: the public key, and~~ a hash of the public key with a temporary secret;

determining whether at least a portion of the certificate request data transmitted to the comparison agent matches the data representative of the public key stored in the storage, and if so:

generating an endorsement certificate at least in part using the public key; ~~and~~

providing the endorsement certificate to the customer device; and

erasing the temporary secret from the security module after the certificate request data has been sent to the comparison agent so that the temporary secret cannot subsequently be discovered.

2. (original) The method of Claim 1, wherein the receiving act is associated with a request from the customer device for the endorsement certificate.

3. (original) The method of Claim 1, further comprising transferring the customer device to a customer after the storing act.

4. (original) The method of Claim 1, wherein the security module is a trusted platform module (TPM).

5. (original) The method of Claim 1, wherein the storage and the comparison agent are not associated with a vendor of the customer device.

6. (original) The method of Claim 1, further comprising signing the endorsement certificate with a signing key.

7 (canceled).

8. (currently amended) A customer computing device, comprising:

at least one security module containing a private key and a public key related to the private key, the keys establishing an endorsement key pair;

at least one processor operatively connected to the security module and executing logic comprising:

requesting an endorsement certificate at least in part by sending data representative of the public key to a source of endorsement certificates, the data representative of the public key including a hash of the public key with a nonce; and

if it is determined at the source that the data representative of the public key matches a version of the data representative of the public key already at the source, receiving from

the source an endorsement certificate generated by the source, the endorsement certificate being generated at least in part using the public key;

wherein the nonce is erased from the security module after the data representative of the public key has been sent to the source so that the nonce cannot subsequently be discovered.

9. (original) The device of Claim 8, wherein the endorsement certificate is signed with a signing key.

10. (original) The device of Claim 8, wherein the security module is a trusted platform module (TPM).

11. (original) The device of Claim 8, wherein the source of endorsement certificates is not the source of the customer device.

12, 13 (canceled).

14. (currently amended) A service comprising:

storing data representative of public keys associated with respective customer computing devices;

receiving transmissions of data representative of public keys from customer computing devices;

comparing the received data representative of a public key with at least the stored data representative of a public key to determine if a match is found; and, if a match is found:

generating an endorsement certificate if a match is found; and

providing the endorsement certificate to the customer computing device, wherein the data representative of a public key includes a hash of the public key and a secret, the secret being erased from the customer computing device after the data representative of the public key has been sent to the facility such that the secret cannot be rediscovered.

15. (original) The service of Claim 14, wherein the endorsement certificate is generated based at least in part on the associated public key.

16. (original) The service of Claim 15, further comprising signing the endorsement certificate with a signing key before providing the endorsement certificate to the customer computing device.

17. (original) The service of Claim 14, wherein the public keys are associated with respective trusted platform modules.

18, 19 (canceled).

20. (currently amended) A computing facility comprising:

means for storing data representative of public keys associated with respective customer computing devices, prior to providing the devices to customers;

means for receiving transmissions of data representative of public keys from devices provided to customers;

means for comparing data representative of a public key received from a device provided to a customer with at least data representative of a public key in the means for storing to determine if a match is found;

means for generating an endorsement certificate based at least in part on the associated public key if a match is found; and

means for transmitting the endorsement certificate to the customer device, wherein the data representative of a public key includes a hash of the public key and a secret, and the secret is erased from a customer computing device after the data representative of the public key has been sent to the facility so that the secret cannot be rediscovered.

21. (original) The facility of Claim 20, wherein the means for generating signs the endorsement certificate with a signing key before transmitting the endorsement certificate to the customer device.

22. (original) The facility of Claim 20, wherein the public keys are associated with respective trusted platform modules.

23, 24 (canceled).